29/9/2015
Russell's course, Lec 10

Hardness from derandomization.

Top event: 1) of Kannan's 1b $\Sigma_3^{EXP} \not\subseteq Size(2^{o(n)})$

b) re-scale: $n^{\omega(1)} \le T(n) \le 2^n$: $\Sigma_3^{T(n)} \not\subseteq Size(T(n)^{O(1)})$; use Kannan's 2n. in Σ_3^P with $n^{O(1)}$ bits

2. Assume $EXP \subseteq P/poly \Rightarrow CAPP \in NTime(2^{n^{O(1)}})$

3) $EXP \subseteq \Sigma_2^P \subseteq \Sigma_3^P \subseteq P^{perm} \subseteq EXP$ (reserve)

BLR, LFKN, c) $Perm \in P/poly \to Perm \in MA$; guess circ, "put it" in prob. poly time. use as oracle.

c) $MA \subseteq NTIME(2^{n^{O(1)}})$; replace "A" with CAPP alg. (prob. can fix)

d) $EXP = P^{perm} = MA = \Sigma_3^P \subseteq NTIME(2^{n^{O(1)}})$

e) rescale: $\Sigma_3^{T(n)} \subseteq NEXP$ for some $T(n) = n^{\omega(1)}$

f.) $\vdots$ #6); $NEXP \not\subseteq P/poly$.

PIT: given an arithm circ, is poly it computes $= 0$?

Say $PIT \in NTIME(2^{n^{O(1)}})$. Either Perm & Ans $P/poly$ or $NEXP \not\subseteq P/poly$.

Assume $PIT \in NTIME(2^{n^{O(1)}})$, $EXP \subseteq P/poly$, $Perm \in Ans - P/poly$.

Same reasoning except mine 2c and 2b: merge into "2b'",

2b') if $Perm \in Ans P/poly$, then $P^{perm} \in NP^{PIT}$

2c') assume also $PIT \in NTIME(2^{n^{O(1)}})$, $P^{perm} \subseteq NTIME(2^{n^{O(1)}})$.

Downward self-reducibility of permanent: expansion by minors.

$Perm(M_{n\times n}) = \sum_{i=1}^{n} M_{i,1} \, Perm(M_{n\times n})_{\not i,1}$; $Perm(M_{1\times 1}) = M_{1,1}$.

- any perm satisfies these equations.

Guess $C_1, \ldots$ as circ C_n = perm on $n\times n$ matrices).

Reduce from this $C_1 \to C_{n-1}$. $(0,1,2)$. Verify $C_i(M) \stackrel{?}{=} \sum_{k=1}^{n} M_{1,k} \cdot C_{i-1}(M_{\not 1,\not k})$

- use PIT to verify, M is a symbolic matrix.

- also gives $P^{perm} \subseteq coNP^{PIT}$.

Natural proofs: Circuit lbs.

A) characterize what circs can compute

B) show some pseudorandom function does not meet property A.

Natural property [RR]. Property $\mathcal{C}(f)$, f given as truth table, $\mathcal{C}(f)$ is true or false: $\underbrace{\square\square\cdots\square}_{2^n}$. Hardness $\mathcal{C}(f)$ is true easy $\mathcal{C}(f)$.

a. $\mathcal{C}$ is constructive $\mathcal{C} \in P = Time(2^{O(n)})$ e.g. $n^{\omega(1)}$

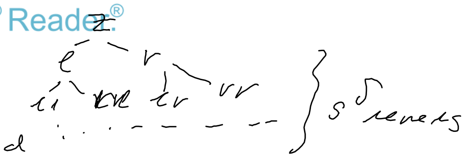
b. $\mathcal{C}$ is useful; if $\mathcal{C}(f)$ is true, then f does not have small circs.

c. $\mathcal{C}$ is large: $Prob(\mathcal{C}(f)) \ge \Omega(1)$

"b is soundness, c is (prob) completeness".

- All lbs so far have natural properties in them.

Cryptographic PRGs: $G: \{0,1\}^s \to \{0,1\}^{2^s}$, and has 2^n security. Then using [GGM] can get $G': \{0,1\}^s \to \{0,1\}^{2^s}$, and, moreover, has random access: given s, i can compute $G'(s)_i$ in poly time



look at S (bits) as a root of a tree: let z be a seed
leaves of the tree are look random.
let $f_z(i) = \hat{G}(z)_i$. $\forall z$, $f_z \in \text{size}(s^{O(1)})$ = size$(|i|^{O(1)})$
- every f_z is easy. But f_z looks random -
$N(f_z)$ = false $\forall z$. But $N(f_R)$ = true whp. But N distinguishes output of $\hat{G}$ from random, contradiction.
If strong enough PRG exist, need to give up some properties.
Let us "give up" some largeness: replace by non-emptiness: "Barely natural"
Assume $\exists$ barely natural property. Then NEXP $\not\subseteq$ P/poly.
(Paraphrase of a version of "easy witness" lemma from IKW02: turns "sometimes" non-empty).
Follow same steps, except for 2c. Alternatively, use the results as black box: show how barely natural property $\Rightarrow$ subexp alg for CAPP.
Lemma: if $\exists$ barely natural property, then can decide CAPP $\in$ NTIME$(2^{n^{o(1)}})$
a) Given an instance of CAPP, set $m = n^\delta$ (inverse of usefulness).
b) Guess a fn f_m s.t. $N(f_m)$ holds, f_m is m-bit Bool fn - $(2^{O(m)}) = 2^{n^\delta}$
size$(f_m) \geq n^{O(1)}$
Use BFNW to construct $G: \{0,1\}^{\text{poly}(m)} \to \{0,1\}^n$ hard for size n
Try all seeds to estimate CAPP.
Easy witness lemma. NEXP: $x \in L \Leftrightarrow \exists y, |y| = 2^{|x|^{O(1)}}$ $R(x,y)$. y witness.
Succinct (easy) witness: described by small circ $C(i) = y_i$.
Easy witness lemma: positive instances of all NEXP relations have easy witnesses iff NEXP $\subseteq$ P/poly.
(One direction: NEXP $\Rightarrow$ easy witnesses, EXP = NEXP $\subseteq$ P/poly).
Other direction: $N_x(y) = R(x,y)$. (only get N_x i.o., need advice) still NEXP $\not\subseteq$ P/...